École polytechnique **M1 d'Informatique**

INF551 : Logique et calculabilité

Composition

Stéphane Lengrand

Lundi 13 Décembre 2010, 3h

L'énoncé fait 3 pages. La barème, sur 24 points, anticipe la possibilité que tous les exercices ne soient pas traités dans le temps imparti. Il est donné à titre indicatif et peut être sujet à légère modification.

Exercice 1 (5 points)

1. Construisez des arbres de preuve (en calcul des séquents) des séquents suivants :
$$\vdash ((p \Rightarrow q) \Rightarrow p) \Rightarrow p$$
$$\vdash ((p \wedge q) \Rightarrow r) \Rightarrow (p \Rightarrow (q \Rightarrow r))$$

Correction :

$$\dfrac{\dfrac{\dfrac{\dfrac{}{p \vdash p, q}}{\vdash p, p \Rightarrow q} \quad \dfrac{}{p \vdash p}}{(p \Rightarrow q) \Rightarrow p \vdash p}}{\vdash ((p \Rightarrow q) \Rightarrow p) \Rightarrow p}
\qquad
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{p, q \vdash r, p} \quad \dfrac{}{p, q \vdash r, q}}{p, q \vdash r, p \wedge q} \quad \dfrac{}{r, p, q \vdash r}}{(p \wedge q) \Rightarrow r, p, q \vdash r}}{(p \wedge q) \Rightarrow r, p \vdash q \Rightarrow r}}{(p \wedge q) \Rightarrow r \vdash p \Rightarrow (q \Rightarrow r)}}{\vdash ((p \wedge q) \Rightarrow r) \Rightarrow (p \Rightarrow (q \Rightarrow r))}$$

2. Soit A la formule $\forall x\ \forall y\ (p(x, y) \Rightarrow p(f(x), f(y)))$.
Quelles sont les variables libres de la proposition A ?
Correction :
L'ensemble des variables libres de A est $\emptyset$.

3. Construisez un arbre de preuve (en calcul des séquents) du séquent suivant :
$$\vdash A \Rightarrow \forall x'\ ((\forall y'\ p(x', y')) \Rightarrow p(f(x'), f(f(x'))))$$

Correction :
Soit B la formule $\forall y'\ p(x', y')$ et C la formule $\forall y\ (p(x', y) \Rightarrow p(f(x'), f(y)))$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A, C, B, p(x', f(x')) \vdash p(f(x'), f(f(x'))), p(x', f(x'))} \quad \dfrac{}{A, C, p(f(x'), f(f(x'))), B, p(x', f(x')) \vdash p(f(x'), f(f(x')))}}{A, C, p(x', f(x')) \Rightarrow p(f(x'), f(f(x'))), B, p(x', f(x')) \vdash p(f(x'), f(f(x')))}}{A, C, B, p(x', f(x')) \vdash p(f(x'), f(f(x')))}}{A, B, p(x', f(x')) \vdash p(f(x'), f(f(x')))}}{A, B \vdash p(f(x'), f(f(x')))}}{A \vdash B \Rightarrow p(f(x'), f(f(x')))}}{A \vdash \forall x'\ (B \Rightarrow p(f(x'), f(f(x'))))}}{\vdash A \Rightarrow \forall x'\ (B \Rightarrow p(f(x'), f(f(x'))))}$$

4. Le séquent ci-dessus est-il prouvable en logique constructive ?
   Correction :
   Oui, les séquents dans la preuve ci-dessus n'ont jamais qu'une seule formule à droite, il n'y a pas de contraction à droite.

Exercice 2 (4 points)

Soit p un symbole de prédicat binaire.

1. On rappelle qu'une formule A est une *conséquence sémantique* d'une théorie $\mathcal{T}$ si tout modèle de $\mathcal{T}$ est aussi un modèle de A.
   Montrer qu'aucune des formules $(R), (S), (T)$ ci-dessous n'est conséquence sémantique de la théorie formée des deux autres formules.

$$
\begin{array}{ll}
(R) & \forall x\ p(x,x) \\
(S) & \forall x\ \forall y\ (p(x,y) \Rightarrow p(y,x)) \\
(T) & \forall x\ \forall y\ \forall z\ ((p(x,y) \wedge p(y,z)) \Rightarrow p(x,z))
\end{array}
$$

   Correction :
   Modèle de $(R), (S)$ qui n'est pas modèle de (T) :
   Univers : les entiers $\mathbb{N}$
   Interprétation de p : $\tilde{p}(n,m) = true$ si $\mid n-m \mid \leq 1$, $\tilde{p}(n,m) = false$ sinon.

   Modèle de $(T), (R)$ qui n'est pas modèle de (S) :
   Univers : les entiers $\mathbb{N}$
   Interprétation de p : $\tilde{p}(n,m) = true$ si $n \leq m$, $\tilde{p}(n,m) = false$ sinon.

   Modèle de $(S), (T)$ qui n'est pas modèle de (R) :
   Univers : les entiers $\mathbb{N}$
   Interprétation de p : $\tilde{p}(n,m) = false$ pour tous n, m.
2. Que peut-on dire d'un modèle validant les trois formules ?
   Donner l'un d'entre eux.
   Correction :
   Un tel modèle est une relation d'équivalence.

   Modèle de $(R), (S), (T)$:
   Univers : les entiers $\mathbb{N}$
   Interprétation de p : $\tilde{p}(n,m) = true$ pour tous n, m.

Exercice 3 : Suite de Fibonacci (7 points)

Soit u_n la suite de Fibonacci définie par

$$
\begin{array}{ll}
u_0 & = 0 \\
u_1 & = 1 \\
u_{n+2} & = u_n + u_{n+1}
\end{array}
$$

1. Donner un système de réécriture qui transforme l'expression $F(n)$ où n est un nombre entier écrit avec les symboles 0 et S en le nombre entier u_n écrit de la même manière.
   L'utilisation de symboles auxiliaires est autorisée.

Correction :

$$\begin{array}{rl}F(0) & \longrightarrow 0\\ F(S(0)) & \longrightarrow S(0)\\ F(S(S(x))) & \longrightarrow \mathsf{Plus}(F(x), F(S(x)))\\ \mathsf{Plus}(0,x) & \longrightarrow x\\ \mathsf{Plus}(S(y),x) & \longrightarrow S(\mathsf{Plus}(y,x)\end{array}$$

2. On rappelle que, pour tous λ-termes M, N et P, $M\ N\ P$ représente $(M\ N)\ P$. Pour tout entier n, $\underline{n}$ dénote le λ-terme de Church représentant n.

   (a) Donner deux λ-termes clos (sans variables libres) K_1 et K_2 tels que : pour tous λ-termes M et N, $\quad K_1\ M\ N \rhd^* M \quad$ et $\quad K_2\ M\ N \rhd^* N$
   Correction :
   $K_1 = \mathit{fun}\ x.\mathit{fun}\ y.x$ et $K_2 = \mathit{fun}\ x.\mathit{fun}\ y.y$

   (b) Pour tous λ-termes clos M et N, (M, N) dénote $\mathit{fun}\ x \to (x\ M\ N)$.
   Donner deux λ-termes clos π_1 et π_2 satisfaisant la propriété suivante : pour tous λ-termes clos M et N, $\pi_1\ (M,N) \rhd^* M$ et $\pi_2\ (M,N) \rhd^* N$
   Correction :
   $\pi_1 = \mathit{fun}\ x.(x\ K_1)$ et $\pi_2 = \mathit{fun}\ x.(x\ K_2)$

   (c) Donner un λ-terme clos plus, tel que
   pour tous entiers m et n, $\mathsf{plus}\ \underline{m}\ \underline{n} \rhd^* \underline{m+n}$
   Correction :
   $\mathsf{plus} = \mathit{fun}\ n.\mathit{fun}\ m.\mathit{fun}\ x.\mathit{fun}\ f.(n\ (m\ x\ f)\ f)$

   (d) Donner un λ-terme clos next, tel que
   pour tous entiers m et n, $\mathsf{next}\ (\underline{m}, \underline{n}) \rhd^* (\underline{n}, \underline{m+n})$
   Correction :
   $\mathsf{next} = \mathit{fun}\ x.(\pi_2\ x, \mathsf{plus}\ (\pi_1\ x)\ (\pi_2\ x))$

   (e) Donner un λ-terme clos aux, tel que pour tout entier n, $\mathsf{aux}\ \underline{n} \rhd^* (\underline{u_n}, \underline{u_{n+1}})$.
   Correction :
   $\mathsf{aux} = \mathit{fun}\ n.(n\ (\underline{0}, \underline{1})\ \mathsf{next})$
   où $\underline{0}$ et $\underline{1}$ sont les entiers de Church $\mathit{fun}\ x.\mathit{fun}\ f.x$ et $\mathit{fun}\ x.\mathit{fun}\ f.(f\ x)$

   (f) En déduire un λ-terme clos fibo, tel que pour tout entier n, $\mathsf{fibo}\ \underline{n} \rhd^* \underline{u_n}$
   Correction :
   $\mathsf{fibo} = \mathit{fun}\ n.(\pi_1\ (\mathsf{aux}\ n))$

Exercice 4 : Machines de Turing à 1 bande (8 points)

Soit Σ un alphabet à deux lettres : blanc (b) et bâton ($|$).

Dans cet exercice on propose de montrer qu'une machine de Turing M à deux bandes sur l'alphabet Σ peut être simulée par une machine M' à une bande sur Σ.[1]

L'idée générale est que les cases paires de l'unique bande de M' vont représenter la première bande de M, et les cases impaires la deuxième bande de M.

1. Ecrire une machine de Turing Init à une bande telle que, si cette bande contient initialement la représentation d'un entier n (une suite de n bâtons suivis d'une infinité de blancs), elle s'arrête en ayant réparti les bâtons une case sur deux : des bâtons dans les cases $2i$ pour $0 \leq i < n$ et des blancs dans les autres cases.

1. Pour aider vos constructions de machines de Turing, vous pourrez considérer qu'à gauche de chaque bande il y a une case, d'indice -1, qui contient un symbole spécial $\times$ indiquant qu'il n'y a plus de cases à gauche ; une machine n'a pas le droit de modifier le contenu de cette case spéciale.

2. On considère une notion de machine de Turing à une bande où les déplacements ne sont pas juste parmi $\{-1, 0, 1\}$ mais plus généralement parmi $\{-2, -1, 0, 1, 2\}$. La notion de petit pas de calcul est adaptée pour que la tête de lecture/écriture se déplace de 2 cases vers la gauche ou vers la droite si la fonction de transition indique -2 ou $+2$.

   Soit M_1 (la fonction de transition d')une telle machine de Turing, avec $\mathcal{S}$ comme ensemble d'état. Montrer qu'en utilisant un ensemble d'états $\mathcal{S}'$ plus grand ($\mathcal{S} \subseteq \mathcal{S}'$), M_1 peut être simulée par une machine M_1' qui n'utilise comme déplacement que $\{-1, 0, 1\}$. [2]

3. Soit $\mathcal{S}$ l'ensemble des états d'une machine de Turing M à 2 bandes et à déplacements dans $\{-1, 0, 1\}$. Nous allons construire une machine M' à 1 bande basée sur une extension $\mathcal{S}'$ de $\mathcal{S}$ où, pour chaque état $s \in \mathcal{S}$, $\mathcal{S}'$ possède s et 4 états supplémentaires, qui représentent intuitivement les situations suivantes :

   s "Je suis sur la case $2i$ et je ne sais pas le contenu de la case $2i + 1$"
   s_1 "Ayant lu b dans la case $2i$ je me suis déplacé sur $2i + 1$ pour lire son contenu"
   s_2 "Ayant lu $|$ dans la case $2i$ je me suis déplacé sur $2i + 1$ pour lire son contenu"
   s_3 "Ayant écrit dans la case $2i + 1$ je me suis redéplacé sur $2i$ pour y écrire b"
   s_4 "Ayant écrit dans la case $2i + 1$ je me suis redéplacé sur $2i$ pour y écrire $|$"

   Voici les 4 types de transitions possibles à partir de s dans la machine M :

$$\begin{array}{ll} M((\mathsf{b}, a), s) & = ((\mathsf{b}, a'), s', d) \\ M((|, a), s) & = ((\mathsf{b}, a'), s', d) \\ M((\mathsf{b}, a), s) & = ((|, a'), s', d) \\ M((|, a), s) & = ((|, a'), s', d) \end{array}$$

   (a et a' sont des lettres quelconques, s' est un autre état de $\mathcal{S}$ et $d \in \{-1, 0, 1\}$)

   Sous forme graphique ou sous forme d'un tableau, donner les transitions correspondantes dans $\mathcal{S}'$ pour définir une machine M' à 1 bande et à déplacement dans $\{-2, -1, 0, 1, 2\}$, qui simule M. [3]

4. Etant donné une machine de Turing M_2 à une bande, montrer comment on peut lui rajouter une deuxième bande de manière à ce que, lorsque la machine s'arrête, cette deuxième bande contient $|$ dans toutes les cases dont la position a été atteinte par la tête de lecture et b dans les cases suivantes.
   (Expliquer comment la fonction de transition de M_2 est adaptée.)

5. Etant donné une machine de Turing M_3 à une bande, on suppose qu'elle s'est arrêtée de manière à ce que :
   - une case d'indice $2i + 1$ contient $|$ si la position $2i$ a été atteinte par la tête de lecture pendant l'exécution de M_3, et contient b sinon.
     (donc si une case $2i + 1$ contient b toutes les cases suivantes contiennent b)
   - la suite des cases d'indice $4i + 2$ représente un entier particulier n
     ($|$ dans les cases $4i + 2$ pour $0 \leq i < n$, b dans les cases $4i + 2$ pour $n \leq i$)
   - les cases d'indice $4i$ ont un contenu que l'on cherche à oublier

   Ecrire une machine de Turing $\mathsf{Cleanup}$ (à une bande) qui commence sur une telle bande et la transforme en la représentation de n (une suite de n bâtons suivis d'une infinité de blancs).

---

2. Pour être formel, on dit que M *est simulée par* M' si la propriété suivante est vérifiée : si M et M' sont dans des situations similaires et M effectue une transition, alors M' se retrouve dans une situation similaire à celle de M après un nombre fini de transitions. Par définition, M et M' *sont dans des situations similaires* si elles sont dans le même état, si leurs bandes contiennent les mêmes données, et si leurs têtes de lecture sont dans une même position.

3. Ici, les bandes de M et M' "contiennent les mêmes données" si pour tout $i \in \mathbb{N}$ la case i de la première bande de M a le même contenu que la case $2i$ de M' et la case i de la deuxième bande de M a le même contenu que la case $2i + 1$ de M'. Leurs têtes de lecture sont "dans une même position" si celle de M' est sur la case $2i$ dès que celle de M est sur la case i.

6. On dit qu'une fonction f de $\mathbb{N}$ dans $\mathbb{N}$ est *représentable par une machine de Turing* M_4 *à 1 bande* si pour tout entier n représenté initialement sur la bande,
   - si f n'est pas définie en n alors M_4 ne s'arrête pas
   - si $f(n) = q$ alors M_4 s'arrête en laissant la représentation de l'entier q sur son unique bande

   Montrer, en combinant les résultats précédents, que toute fonction représentable par une machine de Turing à 2 bandes (au sens habituel) est représentable par une machine de Turing à une bande.